

REDACTED

UNITED STATES DISTRICT COURT

for the

Eastern District of Virginia

In the Matter of the Search of

(Briefly describe the property to be searched)

[REDACTED], Virginia Beach, VA [REDACTED]  
(a white, single-story, detached residence with a  
one-car garage, light colored roof, and the numbers  
"4853" posted on the side of the house)

) ~~UNDER SEAL~~  
) Case No. 2:17sw 38  
)  
)  
)  
)  
)

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location): **See Attachment A**

[REDACTED], Virginia Beach, Virginia [REDACTED] (a white, single-story, detached residence with a one-car garage, light colored roof, and the numbers "4853" posted on the side of the house)

located in the Eastern District of Virginia there is now concealed (identify the person or describe the property to be seized):  
**See Attachment B.**

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section(s)	Offense Description
18 U.S.C. § 1030	Fraud and related activity in connection with computers

The application is based on these facts: **See Affidavit.**

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of \_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

REVIEWED AND APPROVED:

\_\_\_\_\_  
**Randy C. Stoker**  
Assistant United States Attorney

\_\_\_\_\_  
*Applicant's signature*  
  
\_\_\_\_\_  
**Marshall Ward, Special Agent, FBI**  
*Printed name and title*

Sworn to before me and signed in my presence.

Date: \_\_\_\_\_

\_\_\_\_\_  
*Judge's signature*

City and state: \_\_\_\_\_

\_\_\_\_\_  
*Printed name and title*

**REDACTED**

**AFFIDAVIT**



I, Marshall Ward, being duly sworn, depose and state as follows:

1. I am a Special Agent (SA) of the Federal Bureau of Investigation (FBI), and have been so employed since December 2008. I am currently assigned to work cyber and organized crime investigations to include major theft, money laundering, computer intrusions, Internet fraud, wire fraud, bank fraud, and financial institution fraud within the Norfolk, Virginia Division.

2. My experience includes the investigation of cases involving the use of computers and the Internet to defraud, to illegally access computers, and to commit financial institution fraud. I have received law enforcement training in the investigation of criminal violations of federal law within the jurisdiction of the FBI, and have received specialized training in the investigation of computer-related crimes. Additionally, I have received training and gained experience in arrest procedures, search warrant applications, the execution of searches and seizures, and various other criminal laws and procedures. I have participated in the execution of assorted search warrants, including those involving the search and seizure of computers and telephonic devices.

3. The facts and information set forth in this affidavit are derived from my participation in this investigation and the investigation of other law enforcement agents involved with this case, from my review of documents and computer records related to this investigation, and from information gained through my training and experience. Since this affidavit is being submitted for the limited purpose of establishing probable cause, I have not included each and every fact known to investigators about this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to support the issuance of a search warrant.

4. This affidavit supports an application for a search warrant for the following premises within the Eastern District of Virginia:

  
**Virginia Beach, Virginia** 

5. Based upon the information contained in this affidavit, I submit that probable cause exists to believe that:

- a. One or more persons knowingly caused the transmission of a program, information, code, or command, and as a result of such conduct, intentionally caused damage without authorization, to a protected computer, in violation of Title 18, United States Code, Section 1030; and
- b. Evidence, fruits, and instrumentalities (further described in Attachment B) of these offenses will be found at the premises identified in paragraph 4 above (as further described in Attachment A).

### PROBABLE CAUSE

6. On or about September 16, 2014, France's internal security service, DGSJ, contacted the FBI's legal attaché office in Paris to request assistance with a cyber-investigation. DGSJ reported that SFR, one of France's primary Internet service providers (ISPs), had experienced a Distributed Denial of Service (DDoS) attack against its network that lasted from July 27 through August 1, 2013. This caused a disruption that slowed or denied access to servers from legitimate users, which affected the foreign or interstate commerce or communication of the United States.

7. DGSJ's investigation traced the source of the attack to six servers hosted in the Netherlands. DGSJ contacted Dutch authorities, who advised that all six servers were leased by a person in the United States named Adonis Mariano. The Dutch provided Mariano's address as [REDACTED], Abingdon, Maryland [REDACTED] and his telephone number as [REDACTED]-1934. The Dutch further advised that Mariano associated a PayPal account with the leased servers, with an email address of [REDACTED]@yahoo.com.

8. The Dutch authorities also provided DGSJ with relevant log files and copies of the six servers. DGSJ conducted forensic reviews of this evidence, and found indications of approximately 160 additional DDoS attacks, including 51 attacks against ISPs based in the United States. The log files revealed two remote connections into at least one of the servers just prior to the launch of the attack against SFR. The remote sessions originated from IP addresses [REDACTED] and [REDACTED]. DGSJ conducted open source "WHOIS" queries for these two IP addresses, and found that they were assigned to servers hosted by Nuclear Fallout Enterprises (Nuclear Fallout), based in New York, New York. Because Adonis Mariano and the Nuclear Fallout servers were located in the United States, DGSJ requested assistance from the FBI.

9. The FBI opened an investigation to confirm the identity and location of Adonis Mariano, and to determine whether he was responsible for the DDoS attacks in France. Based upon the address provided by Dutch authorities, the case was originally opened in the FBI's office in Baltimore, Maryland.

10. On March 18, 2015, the FBI obtained records from Nuclear Fallout relating to IP addresses [REDACTED] and [REDACTED]. Nuclear Fallout's records indicated that IP address 74.91.116.44 was assigned to a computer server named "Gwapo VPS" (VPS is a common abbreviation for Virtual Private Server), and had been continuously leased from May 8, 2013 through October 21, 2013. Nuclear Fallout indicated that the same user account had continuously leased the server at IP address [REDACTED], from June 13, 2013 through October 3, 2013.

11. The FBI's Baltimore Division conducted Accurant database checks, and found records indicating that Adonis Mariano, with telephone number [REDACTED]-1934, no longer resided in Maryland, and instead lived at [REDACTED], Virginia Beach, Virginia [REDACTED]. On

February 4, 2015, I conducted surveillance at that residence and found a Nissan sedan parked outside, bearing Virginia license plate [REDACTED]. Virginia Department of Motor Vehicles records indicated that the vehicle was registered to Adonis Mariano, with a date of birth of [REDACTED], 1986, and Social Security Account Number of [REDACTED]-4997. Based upon the new location information for Adonis Mariano, the FBI transferred its investigation from Baltimore to Norfolk, Virginia.

12. I conducted additional law enforcement database queries for Adonis Mariano, and found a PayPal account in his name, with a date of birth of [REDACTED], 1986, and a Social Security Account Number of [REDACTED]-4997, which had been used in suspected fraudulent activity.

13. On October 30, 2015, I obtained records from PayPal with information related to Adonis Mariano. PayPal's records indicate he owns several accounts. One of these accounts lists his email address as [REDACTED]@yahoo.com, and his telephone number as [REDACTED]-1934. The account is linked to a credit card number ending in 7223.

14. A second PayPal account in Adonis Mariano's name lists his email address as [REDACTED]@yahoo.com, telephone number as [REDACTED]-1934, and address as [REDACTED], **Virginia Beach, VA** [REDACTED]. This second account is also linked to a credit card ending in 7223, which I verified as being the same credit card account listed in paragraph 13 above. The records for the second account list an online PayPal login history that includes access in 2014 from IP address [REDACTED]. WHOIS records indicate that IP address is provisioned by Verizon FIOS in Virginia.

15. A third PayPal account in Adonis Mariano's name lists his email as address [REDACTED]@yahoo.com, his telephone number as [REDACTED]-1934, and his home address as [REDACTED], Abingdon, MD [REDACTED].

16. A fourth PayPal account in Adonis Mariano's name lists his email as address [REDACTED]@yahoo.com, and telephone number as [REDACTED]-1934. This fourth account is linked to a credit card ending in 0931, and has a login history that includes access in 2010 from IP address [REDACTED]. WHOIS queries indicate [REDACTED] is provisioned by Cox Communications in Virginia.

17. PayPal's fifth account record in the name Adonis Mariano listed his date of birth as [REDACTED], 1986, his Social Security Account Number as [REDACTED]-4997, and his telephone number as [REDACTED]-1934. One of the addresses listed for the account was [REDACTED], **Virginia Beach, Virginia** [REDACTED]. The account is linked to a credit card ending in 0931, which I verified is the same account described above in paragraph 16. This fifth PayPal account record includes alias identifiers for Adonis Mariano, including the moniker "Gwapologist." The following email addresses were listed for the account: [REDACTED]@live.com, [REDACTED]@gmail.com, [REDACTED]@live.com, and [REDACTED]@yahoo.com. This PayPal account lists Adonis Mariano's web site as <http://www.globalmuonline.net>, and links to a bank account at Navy Federal Credit Union named "Gwapo's Virtual Goods Shop."



18. I conducted WHOIS queries for the domain globalmuonline.net, and found that it was registered using email address [REDACTED]@yahoo.com. Further queries of [REDACTED]@yahoo.com revealed that it was also used to register the domain ddoservice.org. I searched online for other information about this domain, and found a posting on Facebook.com, dated August 11, 2012, with the title, "Gwapo's Professional DDOS Service." The posting includes the following statement: "Price starts at 5\$ to 10\$ - 50\$ per hour for ddos protected websites. Payment accepted: Bitcoins / Liberty Reserve / MoneyPak ( US )." The posting lists a "Service Website" of <http://www.ddoservice.org>, and contact email addresses of [REDACTED]@hackforums.net and [REDACTED]@live.com.

19. In order to further identify Adonis Mariano's Internet activity, I conducted additional, iterative online searches. I conducted a WHOIS domain lookup query using the name Adonis Mariano and telephone number [REDACTED]-1934, and found that those identifiers are listed as the registrant for the domain ddosdoesnotexist.com. The record for this registration lists a partial address of Virginia Beach, VA, and a contact email address of [REDACTED]@live.com.

20. I then searched for other domains registered using the email address [REDACTED]@live.com, and found that it was also used to register ddosonline.com. WHOIS queries for this domain list its registrant as "Gwapo Logist," with a partial address of "Virginia Beach." Searches for "Gwapo Logist" indicated that name was also used to register the domain ddossite.com.

21. I researched the domain ddossite.com, and found that as of August, 2015, it automatically redirected users to ddoservice.net. I visited the web page at ddoservice.net, and found that it contained a title of "GWAPO'S PROFESSIONAL DDOS SERVICE." The web page contained links to several online articles about a DDoS service run by a user named "Gwapo." The site claims Gwapo accepts several forms of virtual currency as methods of payment, including Bitcoin, Litecoin and Perfect Money. The page lists various contact methods for Gwapo, including the usernames "gwapooo" on Skype and "gwapologisthf" on Yahoo.

22. On December 30, 2015, I obtained records from Yahoo pertaining to several accounts associated with Adonis Mariano and Gwapo. Upon review of the records returned by Yahoo, I found that the record for [REDACTED]@yahoo.com listed an alternate contact of [REDACTED]@live.com.

23. The Yahoo records also contained information about the account [REDACTED]@yahoo.com. The name associated with the [REDACTED]@yahoo.com account is "Donz Mariano," with a telephone number of [REDACTED]-1934, a zip code of 23464 (Virginia Beach, Virginia), and a date of birth of [REDACTED], 1986. The account was created on April 4, 2010 from IP address [REDACTED], the same Virginia Beach IP address listed in paragraph 16 above. The Yahoo records provided an alternate contact for the account as [REDACTED]@yahoo.com.

24. Next, I attempted to determine where Adonis Mariano's web sites were being

hosted. I conducted Domain Name System (DNS) queries on several of the domains linked to Adonis Mariano, and found that many of them were being hosted by Cloudflare, a provider of virtual hosting services, located in San Francisco, California. For example, the domain ddosservice.net resolves to IP address [REDACTED], and globalmuonline.net resolves to [REDACTED]. I conducted WHOIS queries, and found that Cloudflare hosts both of these IP addresses.

25. On November 9, 2015, I obtained records from Cloudflare pertaining to several of its hosted servers. Upon review of these records, I found that the servers hosting the web sites at ddosservice.org and ddossite.com were both leased by a user with the email address [REDACTED]@live.com. The server hosting the web site globalmuonline.net was leased by an account with two email addresses: [REDACTED]@live.com and [REDACTED]@hotmail.com. The server hosting the web site ddosservice.net was leased by an account with email address [REDACTED]@gmail.com.

26. I conducted internal FBI records checks for "Gwapo" and "ddossite.com," and found that the Albany, New York office of the FBI identified Gwapo as the business partner of a user named "Mystical," who is a subject in one of their investigations. In August, 2015, an FBI employee in Albany logged in with an alias account to the website at Hackforums.net. She located an account for a user named "Gwapo," and reviewed his profile. The profile indicated that Gwapo had logged in to Hackforms.net as recently as August 14, 2015, and listed his homepage as <http://www.ddossite.com>. A review of threads and posts authored by Gwapo indicated that he advertised DDoS and money exchanging services to other users, and sold access to compromised "zombie" computers he controlled, known as "botnets" or "bots."

27. For example, on September 26, 2012, Gwapo authored a thread on Hackforums titled "Gwapo's BOTSHOP INSTALLS FRESH FROM EXPLOIT /BTC/LTC/BTC-E CODE/PM/OKPAY/WMZ/CASHU." In this thread, he listed a contact email address of [REDACTED]@live.com, and advertised the sale of compromised bots and malicious software (malware) installations. Gwapo was active on this thread until November 25, 2014.

28. On October 24, 2014, Gwapo authored another thread on Hackforums titled, "[CHEAP] Gwapo's Professional DDOS Service [ 10\$/hour] [ 200+ Happy Customer Vouches ]." In this thread Gwapo indicated that malware expert James Lyne reviewed Gwapo's DDoS service in a TED Talk presentation titled, "Everyday Cybercrime - And What You Can Do About It." Gwapo also posted a link to the YouTube video of the TED Talk presentation. Gwapo was active on this thread as recently as June 26, 2015, when he posted a comment that the thread was still active.

29. On June 11, 2015, another Hackforums user authored a thread titled, "Help DDOS a Garry's Mod Game Server!" In this thread the author requests assistance in conducting a DDoS attack. On June 12, 2015, Gwapo replied to the request, saying, "contact me if you are willing to pay."

30. On January 29, 2016, I obtained records from Hackforums pertaining to the account named "Gwapo." These records indicate Gwapo associated multiple email addresses with his account since it was opened on September 20, 2011. Gwapo linked the following email addresses to his Hackforums account: [REDACTED]@yahoo.com, [REDACTED]@yahoo.com, [REDACTED]@gmail.com, [REDACTED]@live.com, and [REDACTED]@rogers.com. The records list his current email address as [REDACTED]@gmail.com.

31. The Hackforums records further reveal that Gwapo purchased advertisements or other fee-based upgrades to his account using the following email addresses: [REDACTED]@yahoo.com, [REDACTED]@yahoo.com and [REDACTED]@live.com. Hackforums listed the name using [REDACTED]@live.com as Adonis Mariano.

32. Additional online checks revealed that Gwapo is using videos, social media services and online bulletin boards to publicly advertise his fee-based DDoS services. For example, I found a YouTube user at <https://www.youtube.com/user/Gwapologist>. This user, who titles his YouTube account as "Gwapo DDOS," posted several videos on YouTube. The videos show individuals, who appear to be paid advertisers speaking on behalf of Gwapo, claiming Gwapo can take any server offline. The videos claim Gwapo's fees for conducting DDoS attacks vary, depending on the requested duration of attack, and resources required to conduct the attacks. In one of the videos, posted March 12, 2012, the speaker claims Gwapo uses a Skype username of "gwapooo," and that he can be contacted at any of the following email addresses: [REDACTED]@hackforums.net, [REDACTED]@yahoo.com, or [REDACTED]@live.com.

33. I found that YouTube user "Gwapo DDOS" also posted video recordings of him demonstrating his DDoS attack capabilities. For example, I found a video titled "Gwapo's DDOS Service ( D E M O)," posted on September 30, 2012, that appears to show a real-time DDoS attack against the web sites at <http://awknnet.com> and <http://www.kaspersky.com>. The video shows the web sites loading normally at first, and then becoming unavailable seconds after the attacker initiates his attack.

34. In order to collect first-hand evidence of Gwapo's DDoS attacks. An FBI source was tasked to contact Gwapo through forums online, and to pay Gwapo to conduct a two-hour DDoS attack against a computer operated by a second cooperating FBI source. The attack was planned for May 24, 2016, and on that date I observed the attack in real-time. After logging in to the computer normally, when the attack began I lost complete network connectivity to the computer for almost exactly two hours, as expected.

35. I then attempted to develop additional evidence relating to Gwapo's DDoS service, I obtained records from several email providers relating to his accounts. On June 27, 2016, I received records for the accounts provisioned by Microsoft, including [REDACTED]@live.com. The records contained hundreds of messages that appeared to discuss network DDoS attacks. For example, there were over 200 messages exchanged between 2013 and 2016, with a user using email address [REDACTED]@yandex.com, in which the user requested attacks be directed at several hosts. In a conversation on April 7, 2016, [REDACTED]@yandex.com asked Gwapo to

attack four IP addresses, to which Gwapo responded, "Jus [sic] tested yes we can take them down at the same time." The user then appeared to pay Gwapo for the service, and replied, "1000 USD is now sent to your account. Keep me updated please once attack started and it will be nice if you can send screenshots of results."

36. Review of additional email records indicate that between 2012 and 2016 Gwapo became increasingly concerned about the privacy of his own online identity, and became wary of using PayPal or other traditional banks to accept payments. Complete financial records relating to Gwapo's DDoS services may therefore only be found in computer systems owned or controlled by Gwapo. Furthermore, in many of Gwapo's interactions, he directed the other party to use Skype or instant messaging services to communicate. Records of these conversations are not usually stored on remote servers, and if they exist, may only be found through examination of the computers Gwapo used for the communications.

37. In February, 2017 I re-checked Department of Motor Vehicle records for Adonis Mariano. Current records list his address as [REDACTED], Virginia Beach, Virginia [REDACTED]. The records show he owns a 2014 Nissan sedan with Virginia tag [REDACTED]. On February 22, 2017, I conducted drive-by surveillance of [REDACTED], Virginia Beach, Virginia [REDACTED], and found a 2014 Nissan sedan with Virginia tag [REDACTED] parked in front of the residence.

38. I submit that there is probable cause to believe that Adonis Mariano has had significant involvement in conducting Distributed Denial of Service attacks against various computer networks around the world. I further submit that there is probable cause to believe that Mariano's computers and electronic devices will contain correspondence, financial records and other evidence of his activities, and that these devices will be found in Adonis Mariano's residence at [REDACTED], Virginia Beach, Virginia [REDACTED].

#### **PREMISES AND ELECTRONIC DEVICES TO BE SEARCHED**

39. I seek a warrant to search the premises located at [REDACTED], Virginia Beach, Virginia [REDACTED].

40. I have experience investigating various criminal offenses, which make use of computers and the Internet, telephones, smartphones, and various handheld electronic devices. Based upon my training and experience, I know that such devices and instrumentalities are used, among other ways, to process and store records relating to criminal activity, including making online threats. Individuals engaged in such crimes also commonly use various communication instrumentalities and networks, including the Internet, computers, and cellular telephone networks, to communicate their threats and discuss them with others.

41. From my training and experience and from my discussions with forensic examiners and other investigators, I know that electronic records and information may remain upon computers, cellular or wireless telephones, and associated hard drives, memory, and electronic storage media for an indefinite period of time. For example, cellular telephones usually contain a



“call log,” which records the telephone number, date, and time of calls made to and from the phone. Additionally, based on my training and experience, I know that cellular telephones, such as iPhones and Android smartphones, now offer a broad range of capabilities. These capabilities include, but are not limited to: storing names and numbers in electronic address books; sending, receiving, and storing text and other messages and email; taking, sending, receiving, and storing still photographs and videos; storing and playing back audio files and voicemail messages; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Some cellular telephones also include global positioning system (GPS) technology and data for determining the location of the device at past dates/times. Many cellular telephones now may also be “synced” to a personal or laptop computer, allowing the user to back up the data stored on the phone to a user’s computer.

42. From my training and experience and from my discussions with forensic examiners and other investigators, I also know that computers and cellular telephones, such as iPhones and Android smartphones, store data, both on removable media (for example, CDs, DVDs, thumb drives, memory cards, SIM (subscriber identity module) cards, etc.) and internal media and memory, in ways that are not completely known or controlled by most users. In other instances, users themselves backup data stored on computers, cellular telephones, and other media to protect against its loss, in the event of a malfunction or other event. Once stored, data is usually not destroyed until it is overwritten. For example, data that is “deleted” by a user is usually not actually deleted until it is overwritten by machine processes (rather than user decision) that decide where to store data and when overwriting will occur. Therefore, files and fragments of files and other data may easily last months, if not years, if the storage media is retained. Wholly apart from user-generated files, computer and electronic storage media—in particular, internal hard drives—contain electronic evidence of how a device has been used, what it has been used for, and who has used it. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. Because this information often may be used to establish how computers and other electronic devices were used, the purpose of their use, and when they were used and by whom, I seek permission to search for and seize such evidence, as well as other, more direct evidence of the crimes noted in this warrant. Through the use of proper forensic techniques such data and evidence of criminal offenses may be recovered, notwithstanding the passage of time since a crime occurred.

43. I also know and have been advised by forensic examiners and other investigators that searching and seizing information from computers and electronic devices often requires agents to seize most or all computers and electronic storage devices (along with related peripherals and input/output devices, software, software documentation, and data security devices and passwords), to be searched later by a qualified examiner in a controlled setting. This is true because of: (1) the volume of data contained in computers and various electronic communication and storage devices (like hard disks, diskettes, compact disks, memory chips, and other drives that may be connected to a computer); and (2) the technical processes involved in analyzing computer and other communication systems and devices, storage devices, and their data. Computer storage devices and other media can easily store the equivalent of hundreds of thousands of pages of information (for example, a single gigabyte of storage space is approximately equal to hundreds of thousands of pages of text). To document and to authenticate such data, and to prevent its loss either from accidental or deliberate destruction requires analysis by a qualified examiner in a

controlled environment. Such analysis often requires the seizure, for example, of all of a computer system's hardware and software, peripheral input/output devices, software documentation, and data security devices (including passwords) so that the system or device in question may be properly re-configured and the data contained therein may be accurately retrieved.

44. In addition to the reasons noted above, because computer storage devices, electronic devices, and storage media are instrumentalities used to commit the crimes described in this affidavit, I seek to seize and to conduct an off-site search of same for evidence of the crimes under investigation. Such action will diminish the intrusion of law enforcement into the premises to be searched and will ensure that evidence can be searched for without the risk of losing, destroying, or missing the information/data sought to be seized pursuant to any warrant. Seizure will also preserve such items for later possible later forfeiture, provided they contain contraband or were used as instrumentalities of the crimes under investigation.

### CONCLUSION

45. I submit that the information contained in this affidavit establishes probable cause to believe that:

- a. One or more persons knowingly caused the transmission of a program, information, code, or command, and as a result of such conduct, intentionally caused damage without authorization, to a protected computer, in violation of Title 18, United States Code, Section 1030; and
- b. Evidence, fruits, and instrumentalities (further described in Attachment B) of these offenses will be found at the premises identified in paragraph 4 above (as further described in Attachment A).

46. Accordingly, I request the issuance of a warrant authorizing FBI agents, with the assistance of other law enforcement agencies, to search [REDACTED], Virginia Beach, Virginia [REDACTED].

47. To protect law enforcement officers executing the warrant, to ensure that evidence is not destroyed by any target of the investigation, and to avoid identifying the target of the investigation before any charges are brought, it is requested that this affidavit and accompanying application and search warrant be sealed until further Order of the Court. Premature disclosure of the contents of this affidavit and related documents may have a significant and negative impact on the continuing investigation and may jeopardize its completion and effectiveness.

---

Marshall Ward  
Special Agent  
Federal Bureau of Investigation

Subscribed and sworn to before me this \_\_\_\_ day of March 2017, in Norfolk, Virginia.

---

UNITED STATES MAGISTRATE JUDGE